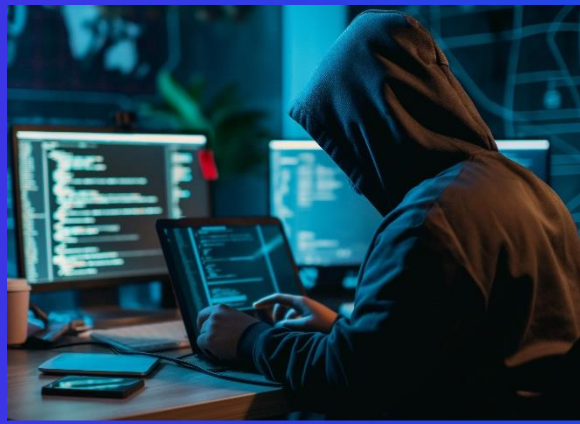
KPMG

KPMG Cyber Threat Intelligence Platform

UNC1860 - A Deep Dive into Their Custom-Built Arsenal

TLP : Clear

KPMG. Make the Difference.



UNC1860 is an Iranian state sponsored threat actor believed to be linked to Iran's Ministry of Intelligence and Security (MOIS), known for acting as an initial access provider and its capability to provide access into government networks across the Middle East. First detected in July 2022 in Albania, was observed deploying malware, backdoors and wipers. A distinguishing feature of UNC1860 is their arsenal of custom-built tools like TEMPLEPLAY and VIROGREEN, GUI-based malware controllers which allow them to infiltrate victim networks via RDP.

Initial access into victim networks is gained by exploiting vulnerabilities in internet-facing servers and utilizing a set of passive, listener-based utilities. After gaining foothold, they deploy custom droppers/web shells to maintain remote access. They utilize custom Base64 and XOR obfuscation methods and rename strings and function names to evade detection. Instead of a traditional C2 infrastructure, they implement utilities and passive implants that are stealthier than traditional backdoors. The network traffic is also encrypted using HTTPS. The C2 uses two malware controllers which provide post-exploitation capabilities such as command execution on host's machines, upload or download files. TEMPLEPLAY can use infected machines as a middlebox using RDP. VIROGREEN scans and exploits CVE-2019-0604 in Sharepoint servers. It also controls post-exploitation payloads. Further, backdoors are deployed which establish persistence using service registries. Backdoors such as TEMPLELOCK can terminate Windows Event Log service threads. The threat actor may scan IP addresses using the victim network, potentially to conduct additional scanning and exploitation activities.

Organizations should patch internet-facing servers to eliminate vulnerabilities and use advanced threat detection to identify hidden malware and custom encryption methods.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

KPMG

KPMG Cyber Threat Intelligence Platform

UNC1860 - A Deep Dive into Their Custom-Built Arsenal

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
1176381da7dea356f3377a59a6f0e799
41f4732ed369f2224a422752860b0bc5
4029bc4a06638bb9ac4b8528523b72f6
126bc1c30fba27f8bf67dce4892b1e8c
0c9ff0db00f04fd4c6a9160bffd85a1d
a7693e399602eb79db537c5022dd1e01
d9719f6738dbfaa21be7f184512fe074
17b27e6aa0ab6501f11bb4d2e0f829ff
4dd6250eb2d368f500949952eb013964
69fd67c115349abb4a313230a1692642
7f5f5f290910d256e6b012f898c88bf3
c90ec587e3333dabb647ebc182673460
efe8043e1b4214640c5f7b5ddf737653
a90236e4962620949b720f647a91f101
b26d54b7da7b2bf600104f69da4ea00f
d87ca3f830b8b53fde358bb64900f6af
c50ae2c4b76f0d5724ec240568c78c4f
57cd8e220465aa8030755d4009d0117c
4b2c78bb2c439998cff0cc097a14b942
4abcf21b63781a53bbc1aa17bd8d2cbc
a3ea0d13848a104c28d035a9d518acc2
bd6464f12bb6f7f02b6ffebb363d8e5f
f89be788e4adf665acf1a8ef8fcaa133
f292e61774c267c3787fdfcace50ea7b
ec238353f020243758eb7511dddf8ab6ba01b35d
4c75085d2d04f7ebda1e459d68dc8a903fa6b459

Indicators of Compromise: Hashes
59026092f2979569b81b0723cc13208dcb4be6f9
9521128269ea6c49476301739257dde9f0a2dbe6
6ec0c1d6311656c76787297775a8d0cb0aa6c4c7
70bc7b43e119060dce54568a1beb140da565a482
2df9c309e08140e9e9af624a6c40355819a91720
79d0f30aab90da8290b8f15703ccf522f2464d7a
a84ab1f4a6860a3b01aa681e1f54c6cb181868e8
c31288e197847ccb0cd66f31c3956f892b0854de
d85e72ba39e0057925f778ae2b12ecd1e245221e
dba1dce5bfe4e0290bd378a0126492569bdabc39
f51b22835a18bc1e7c973ae76c67a3b0299a6487
eb60ffb03e1da380563e796b867fbddeb1fac77d
398ee9da244c53a136efee5e1d8acd1298008497
9c58ec8f7ce75ba1b629c9ef84ab069a32313288
2efd9c5a71decf3787a1fafec7740d2b49b6250c
8182fd937c090675eef1345f95ca2b683361240c
bae8a6aa23c972661063c45cc26a52300f76bb00
8a150ff56027634dd48fe3c9e3dac6ab992ad052
935880fd819dec7b64969b250715f2ec05876b42
84713e84457767b0d4e06c689db4f43d5739c7b4
27f59c451fc3de423bed1176833573435a73b9f7
45cdc9c2b260657f7bd1f194987e14949f3e241d
c0afb5797e6873bbee69f9bf0aa7a9dd3a1c6fff
15db197d98b02d715c15955b0d58d8785ebc750f
9b29d3a718acf5a8a3dd415aa540618d9d114a15
b4e60fea91c014009a3714755fef74d51d55628c

KPMG Cyber Threat Intelligence Platform

UNC1860 - A Deep Dive into Their Custom-Built Arsenal

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
0c6a22dc842c9757b197a8c1aff6757486f97f46
d2d6cddb83b481993d67a85429e3a4af0b466d09
c5b4542d61af74cf7454d7f1c8d96218d709de38f94ccfa7c16b15f726dc08c0
90b3f7fefe8e11b8eacaba09a3c14ed6aa66a4c8d798440d912d0a663917a265
ce59bbe3ef7e16423718de50639d2278eab9c1f08f998677ba6fbd36695f316a
f4639c63fb01875946a4272c3515f005d558823311d0ee4c34896c2b66122596
36b61f94bdfc86e736a4ee30718e0b1ee1c07279db079d48d3fe78b1578dbf03
2538767f13218503bccf31fccb74e7531994b69a36a3780b53ba5020d938af20
b66919a18322aa4ce2ad47d149b7fe38063cd3cfa2e4062cd1a01ad6b3e47651
ed3745f82c7873adca16833b718e20090ac6a8c74e7004b854af29ef1551de75
f6c316e2385f2694d47e936b0ac4bc9b55e279d530dd5e805f0d963cb47c3c0d
8fdd00243ba68cadd175af0cbaf860218e08f42e715a998d6183d7c7462a3b5b
8e4f7a19b09e118ebda79726bf17e9d37ff4b66f4143762dd97ca80340388963
7a1fee8d879bc16e63d05c79c5419bd19ee308c54831d7ee196cfa8281498a06
ff51aa6cad655ddd99a525b78419cd746453fb2adcb689ba34ca3ab6e78b1347
1485c0ed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1c00c780419a4e
58cb1ef132fbdd1855f75c2886666275d1bb75a9fb3fed88d05feee4230afd32
1786916c1e3b16ce654497861fe43bb595ea0f0fa0fad4cd62f3edc82f9a27d4
e1ad173e49eee1194f2a55afa681cef7c3b8f6c26572f474dec7a42e9f0cdc9d
daa362f070ba121b9a2fa3567abc345edcde33c54cabefa71dd2faad78c10c33
359d826ff025c5e4971d90be0d7dfebe10fc125f6dcaa2f0e9869e9f6bec4432
0969f7f5556e3babd7050308a29fa2987dce01b3c94959724c9cd49bce052d80
a375f98aa21377ed0c59b4c7121ac93763157e39d8235fb5ce77f88dee0e2ee4
a650a90c1b505989b7e81bfb310d7e2013a380ab26f99622de158c58b1d0fbbf
3875ed58c0d42e05c83843b32ed33d6ba5e94e18ffe8fb1bf34fd7dedf3f82a7
6f938caeefa0aea3b8301e07bf918a49408cd319187d05ac519b20a00f460469

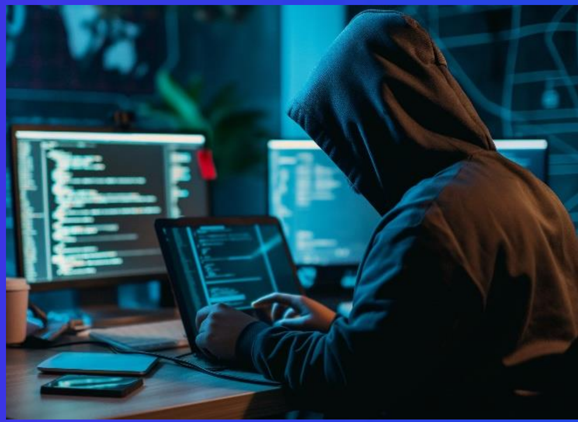
KPMG

KPMG Cyber Threat Intelligence Platform

UNC1860 - A Deep Dive into Their Custom-Built Arsenal

TLP : Clear

KPMG. Make the Difference.



Indicators of Compromise: Hashes
8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330
59463257c3f2425109fd097f814b6468663df947de8178c8cd7b7c5e94d3375c
2097320e71990865f04b9484858d279875cf5c66a5f6d12c819a34e2385da838
e26fbbeea2e152b3769126714c52112d04c4f2310461fb842bf2532e7903ce51
67560e05383e38b2fcc30df84f0792ad095d5594838087076b214d849cde9542
1146b1f38e420936b7c5f6b22212f3aa93515f3738c861f499ed1047865549cb
b65bcba449d74e4395421aeb4012c9e509acb5e8153ff3dc9f01fd97a5cc2711
ac7b01e01de0dc289cd649aa5072243f2036bd8d2d0152b6d9874c2ccaaf1e5d
c0dc609e6fc8801bb902d14910c3ffd69d6bd5a26389836446dc4c23565ddcc7
ffb6acd2715dd988fe3c3fdbd7d45159f8e5b529eea506a856109a8696e93a80
596b2a90c1590eaf704295a2d95aae5d2fec136e9613e059fd37de4b02fd03bb
6f0a38c9eb9171cd323b0f599b74ee571620bc3f34aa07435e7c5822663de605
3269de107e436a75a8308377709dc49b4893cfd137a3fc5b92d0f0590af4cb12
a2598161e1efff623de6128ad8aafba9da0300b6f86e8c951e616bd19f0a572b
da450c639c9a50377233c0f195c3f6162beb253f320ed57d5c9bb9c7f0e83999
786298c0d98aaf35777738a43a41546c6c8b1972b9bd601fb6cccf2c8f539ae4
159eecbba87a7397a5b84a21c289ae66ec776a3fd3b41bf11549fb621afebc0a
1c57b1ed990a8946e86d69da2a047fa15525d883b86e93cb6444a4065dbad362
9117bd328e37be121fb497596a2d0619a0eaca44752a1854523b8af46a5b0ceb
fa2c5fa2814d4db288bf8733edc4f1a78cd2c72cde90f42cf5b14162ac648042
c3fa9432243e1a2ab1991ab4c07a19392038e6a8e817e5fea0232c4caabbb950
e984b40c4c6909813ed9f0ea5de8f4f7cac40f0e8b9fb5041f4a568e307e5712
9483f5eb9133c353cef636ef9fcc29e2c7bf658881574211ee142c93c523efaf
ba3efa7d61e79cf62eeb0c65e803a6353f3012a89e0d910c2292801da43c8a93